Amendments to the Claims:

Amendments to the claims are reflected in the following listing, which replaces any and all prior versions and listings of claims in the present application:

Claim Listing

1. (Currently Amended) A method for conducting a transaction using facilitating biometric security in a smartcard transaction system having a biometric security device, said method comprising:

communicating with a smartcard, wherein said smart card comprises a common application and a second application, said second application storing travel-related information associated with a cardholder, said second application comprising a common file structure and a partner file structure;

determining if when a transaction violates a preset transaction limitation;

notifying a user to proffer a first biometric sample and a second biometric sample to verify an identity of said user;

detecting a proffered biometric sample at a sensor communicating with said system;

generating data representing said proffered biometric sample;

using said data representing said proffered biometric sample as a variable in an encryption calculation to secure at least one of user data and transaction data;

verifying said proffered biometric sample; and

authorizing said transaction to proceed upon verification of said proffered biometric sample.

receiving a first proffered biometric sample and a second proffered biometric sample, wherein said first proffered biometric sample is a different type of biometric sample from said second proffered biometric sample, and wherein said first proffered biometric sample and said second proffered biometric sample are from the same user, and wherein said first proffered biometric sample is required to access said common file structure and said second proffered biometric sample is required to access said partner file structure;

verifying said first proffered biometric sample and a second proffered biometric sample;

enabling write access to a field within said partner file structure upon verification of said second proffered biometric sample and upon request by a first partnering organization;

denying write access to said field upon request by a second partnering organization;

enabling write access for said first partnering organization and said second partnering organization to a field in said common file structure, upon verification of said first proffered biometric sample;

transferring common data to facilitate said transaction; and,

transferring said travel-related information, information related to said common file structure and information related to said partner file structure to facilitate said transaction.

2.   (Currently Amended) The method of claim 1, wherein said step of determining ~~if~~ when said transaction violates said preset transaction limitation includes determining ~~if~~ when said transaction is at least one of a purchase exceeding an established per purchase spending limit, a purchase exceeding a preset number of transactions, any portion of a purchase using non-monetary funds, and a purchase exceeding an established limit.

3.   (Previously Presented) The method of claim 1, wherein said step of notifying includes providing notification by at least one of an audible signal, a visual signal, an optical signal, a mechanical signal, a vibration, blinking, signaling, beeping, providing an olfactory signal, providing a physical touch signal, and providing a temperature signal to said user.

4.   (Currently Amended) The method of claim 1, ~~wherein said step of detecting further includes detecting said proffered biometric sample at said sensor communicating with said system via at least one of a smartcard, a reader, and a network~~ further comprising using data representing said first proffered biometric sample and said second proffered biometric sample as a variable in an encryption calculation to secure at least one of user data and transaction data.

5.   (Cancelled).

6.   (Currently Amended) The method of claim ~~5~~ 1, further comprising accessing card-holder preferences relating to at least one of rental cars, hotel reservations, and air travel in said ~~first~~ partner file structure, upon verification of said first proffered biometric sample and said second proffered biometric sample.

7.   (Currently Amended)   The method of claim 1, further comprising using ~~said~~ data representing said ~~proffered biometric sample~~ first proffered biometric sample and said second

<u>proffered biometric sample</u> as at least one of a private key and a public key to facilitate encryption security associated with said transaction.

8.   (Currently Amended)   The method of claim 1, further comprising using ~~said~~ data representing said ~~proffered biometric sample~~ <u>first proffered biometric sample and said second proffered biometric sample</u> in generating a message authentication code.

9.   (Currently Amended)   The method of claim 1, wherein said step of verifying includes comparing ~~said~~ ~~proffered biometric sample~~ <u>said first proffered biometric sample and said second proffered biometric sample</u> with a stored biometric sample.

10.   (Currently Amended)   The method of claim 9, wherein ~~comparing said proffered biometric sample with said stored biometric sample includes comparing said proffered biometric sample with a~~ <u>said stored</u> biometric sample ~~of~~ <u>is from</u> at least one of a criminal, a terrorist, and a cardmember.

11.   (Currently Amended)   The method of claim 1, wherein said step of verifying includes verifying ~~said~~ ~~proffered biometric sample~~ <u>said first proffered biometric sample and said second proffered biometric sample</u> using information contained on at least one of a local database, a remote database, and a third-party controlled database.

12.   (Currently Amended)   The method of claim 1, further comprising using ~~said~~ data representing ~~said~~ ~~proffered biometric sample~~ <u>said first proffered biometric sample and said second proffered biometric sample</u> to provide substantially simultaneous access to goods and initiation of authentication for a subsequent purchase of said goods.

13.   (Cancelled).

14.   (Currently Amended)   The method of claim 1, further comprising ~~a step of~~ ~~requiring~~ <u>requesting said user to submit</u> ~~submission of~~ a personal identification number <u>and verifying said personal identification number.</u> ~~at said biometric sensor after said step of verifying said proffered biometric sample and before said step of authorizing said transaction to proceed.~~

15.   (Currently Amended)   The method of claim 1, further comprising facilitating a selection of an account from at least two accounts ~~to facilitate said step of authorizing said transaction~~.

16.   (Cancelled).

17.   (Currently Amended) The method of claim 1, further comprising requiring a ~~second~~ third proffered biometric sample to override said preset transaction limitation.

18.   (Cancelled).

19.   (Cancelled).

20.   (Currently Amended) The method of claim 1 ~~5~~ , further comprising writing to at least one of said partner file structure and said common file structure to program said smartcard as a room key.

21.   (New) The method of claim 1, further comprising:

        storing, by a first enterprise data collection unit, update transactions and pending transactions associated with said smartcard and a first enterprise, wherein said first enterprise data collection unit is associated with a first enterprise;

        storing, by a second enterprise data collection unit, update transactions and pending transactions associated with said smartcard and a second enterprise, wherein said second enterprise data collection unit is associated with a second enterprise;

        interfacing with said smartcard and said first and second enterprise data collection units, at an access point;

        storing, by a card object database system coupled to said first and second enterprise data collection units, said smartcard information in accordance with said update transactions and said pending transactions, wherein said smartcard information includes a card object having an application;

        routing, by an update logic system, said smartcard information from said first and second enterprise data collection units to said access point in order to effect synchronization of said smartcard information associated with said smartcard and said card object database system; and,

        activating, by said verification device, said update logic system upon verification of said first proffered biometric sample and said second biometric sample.

22.   (New) The method of claim 21, further comprising securely routing, by an update logic system, card information between said enterprise data synchronization interface and said

enterprise data collection units, wherein said update logic system is coupled to an enterprise data synchronization interface, and communicating, by said enterprise network, with said access point, wherein said enterprise data synchronization interface is coupled to said enterprise network.

23.   (New) The method of claim 22, further comprising, by a secure support client server, communicating with said access point, and adaptively providing communication functionality in accordance with the communication functionality available at said access point.

24.   (New) The method of claim 23, further comprising:

communicating, by a key system, with a security server and supplying a key in response to a request from said security server, wherein said key system is associated with said application;

receiving, by a personalization utility, said card object and communicating with said security server;

adding, by said personalization utility, said key to said card object;

accepting, by a card management system, a card request and communicating said card request to said personalization utility; and

communicating, by a gather application module, with said card management system and gathering application information from a first database and a second database in accordance with said card request, wherein said first database is associated with said first enterprise, and said second database is associated with said second enterprise.

25.   (New) The method of claim 1, further comprising displaying a first plurality of financial accounts upon verification of said first proffered biometric sample, and displaying a second plurality of financial accounts upon verification of said second biometric sample, wherein said first plurality of financial accounts include different financial accounts than said second plurality of financial accounts.

26.   (New) The method of claim 1, further comprising associating a first set of rules with said first proffered biometric sample and displaying a first plurality of financial accounts upon verification of said first proffered biometric sample and said first set of rules, and associating a second set of rules with said second proffered biometric sample and displaying a second plurality

of financial accounts upon verification of said second biometric sample and said second set of rules, wherein said first plurality of financial accounts include different financial accounts than said second plurality of financial accounts.